2016

An assessment of the ICT Security Skills in the Industrial Sector as Provided Through Education and Training

Harald Gjermundrød
University of Nicosia, gjermundrod.h@unic.ac.cy

Ioanna Dionysiou
University of Nicosia, dionysiou.i@unic.ac.cy

Marianne Baumberger
Inno TSD France, m.baumberger@innogroup.com

Marc Pattinson
Inno TSD France, m.pattinson@inno-group.com

AN ASSESSMENT OF THE ICT SECURITY SKILLS IN THE INDUSTRIAL SECTOR AS PROVIDED THROUGH EDUCATION AND TRAINING

Completed Research

Gjermundrød, Harald, University of Nicosia, Nicosia, Cyprus, gjermundrod.h@unic.ac.cy

Dionysiou, Ioanna, University of Nicosia, Nicosia, Cyprus, dionysiou.i@unic.ac.cy

Baumberger, Marianne, Inno TSD France, Sophia-Antipolis, France, M.Baumberger@inno-group.com

Pattinson, Marc, Inno TSD France, Sophia-Antipolis, France, M.Pattinson@inno-group.com

Abstract

Cybersecurity has become an increasingly important aspect of public policy as Internet traffic increases and mounting cyber threats affect the operation of governments and businesses as well as the everyday life of citizens. Cybersecurity policy-making is at a turning point, becoming a national policy priority with explicit strategies in several countries. Even though the availability of high-level ICT security skills would significantly contribute in leveraging the economic growth of companies, still there is a lack of ICT security skills in Europe. In this paper, the ICT security skills gap between the industry needs and the academia/training curricula is investigated in seven European regions, followed by an analysis of the findings. Based on the findings, a framework is proposed to narrow the security skills gap.

Keywords: ICT Security Skills, Education, Training, Curriculum Development.

1 Introduction

Cybersecurity has become an increasingly important aspect of public policy as Internet traffic increases and mounting cyber-threats affect the operation of governments and businesses as well as the everyday life of citizens. Cybersecurity policy-making is at a turning point, becoming a national policy priority with explicit strategies in several countries. Understanding and interacting within a secure and trustworthy digital environment is of benefit to all European citizens and enterprises. Providing awareness and training for citizens may also help citizens to engage with technology and use it to their advantage earlier, with a potential effect of sparking interest in ICT and cybersecurity related careers. Even though the availability of high-level ICT security skills would significantly contribute in leveraging the economic growth of companies, still there is a lack of ICT security skills in Europe. As a matter of fact, according to the $(ISC)^2$ Global Information Workforce Study (Suby and Dickson, 2015), the workforce will grow at a compound annual growth rate of 11.3% globally up to 2017, calling for an additional 2 million new workers. However, there is an ever-widening gap between the supply of qualified information security professionals and the demand for skilled workers to secure critical information and the cyber world. As a result, several hundred thousand ICT-related job vacancies remain unfulfilled.

The educational sector and industry have to closely collaborate to satisfy security demands in this rapidly changing field. The objectives of the present investigation are twofold: Identify missing ICT security competences for the industry at national/regional level across selected European regions and suggest a framework to narrow the ICT security competence gap. The rest of the paper is organized as follows. Section 2 describes the industry trends related to ICT security competences along with the ways that academia incorporates them in its curricula. Section 3 presents the findings of the investigation on the ICT security skills gap, covering several European regions. Section 4 discusses the principles of a framework that could be utilized by regions to narrow the gap. Section 5 concludes the paper.

2 ICT Security Competences Trends

To become innovative and competitive, an economy needs a workforce with the relevant competences, in line with the market and sector trends. Today with the digital transformation, companies have to rapidly and efficiently design or adopt new technologies, and have to modify their way of doing business: ICT skills and competences are essential for driving innovation and business growth. Thus, ICT skills and competences are therefore a major policy concern in Europe to reach the Europe 2020 strategy and its objective of smart, sustainable and inclusive growth.

According to Business Review Europe (Wadlow, 2015), the list of the top 10 IT skills in demand worldwide in 2015 includes cloud security (listed as the top skill), ethical hacking, secure coding, and network penetration. These skills are directly linked to security competences. This outcome in itself is not surprising: in a world where the virtual world increasingly impacts the real world, our growing dependence on Internet technologies and the interdependence between critical resources and infrastructures and connected technologies raise important security issues. The Global Risk 2014 report from the World Economic Forum (World Economic Forum, 2014) identifies cyberattacks, infrastructure disruptions, and data loss (fraud, theft) as the three main technological risks faced by the world. It points out that organizations are faced with a growing volume of cyberattacks: in 2013, there was a 62% increase in the number of security breaches, and 2.5 billion records had been exposed in the last five years as a result of a breach.

The frequency and sophistication of cyberattacks are only going to increase, thus making cybersecurity positions a priority within organizations. Organizations need to put in place effective policies that speak to corporate boards, managers and employees at all levels and at the same time, they need to have the staff who know how to use the existing tools (there are cyber intelligence tools capable of

tracking and alerting on the latest vulnerabilities) and who really understand the threats and their consequences, especially responding to live attacks in real world situations. However, studies conducted worldwide and at the European level demonstrate a clear lack of skilled security experts entering the market, and a dire lack of investment in training: all competent authorities agree that there is a major and growing IT security skills shortage that will impact on economic growth and the competiveness of European businesses. According to Cisco 2014 Annual Security Report (Cisco, 2014)**,** approximatively 1 million of IT security jobs worldwide are unfilled. In a 451 Research Q2 2015 study (Kennedy, 2015), based on responses from over 1,000 IT professionals, primarily in North America, Europe, the Middle East and Africa, security managers reported significant obstacles in implementing desired security projects due to lack of staff expertise (34.5%) and inadequate staffing (26.%). Given this challenge, only 24% of enterprises have 24×7 monitoring in place using internal resources. Finally, according to a Rand Corporation study (Libicki, et al. 2014), there are around 1,000 top-level cyber security experts globally for a need of 10,000 to 30,000.

It is important to know the exact skill sets that are in highest demand, in order to be useful and of use to practitioners and those in a position to alter the situation. The field of IT security is not monolithic, but it is made up of a variety of skill sets involving a combination of technical, planning, and managerial skills. The Global Information Workforce Study (Foster and Sullivan, 2013) conducted an analysis to identify the skill sets most needed by organizations, amongst a list of 39 job categories, inspired from the EU framework of IT Security skills (Pauna, et al., 2014) and the USA National Initiative for Cybersecurity Education (NICE). The results of this survey, and similar ones, can be used to help define educational and training content. They can also help cyber security firms design service offers to meet the needs of other businesses.

Security competences are addressed in academic curricula. There are three major global professional organizations that are representing the computing interests of their members, namely: ACM (Association for Computing Machinery), IEEE (Institute of Electrical and Electronics Engineers), and AIS (Association for Information Systems). There is collaboration among these societies and their curricula committees regularly release curricula guidelines to programs in the ICT domain for higher education institutions. Universities are free to follow the recommendations and it is highly recommended to take them into consideration when programs and/or courses are developed/upgraded. In addition, textbooks often follow the recommendations proposed by the societies for a specific course. The different organizations collaborate on their development with the ACM/IEEE Computer Society being the most active collaboration. The ACM and IEEE Computer Society have collaborated (since 1968) in developing curriculum guidelines released at regular intervals for the computer science field. As the filed has expanded, recommendations for new areas have been forked off into their own recommendation like computer engineering and software engineering. One major change in the latest iteration of the recommendation for the Computer Science (CS2013) undergraduate recommendation was the inclusion of a new *knowledge area* (KA), ***Information Assurance and Security***, which indicates the importance of security in education for the next generation of ICT professionals. Ronald C. Dodge (Dodge, 2013) gives a detailed explanation of the inclusion of this new KA into the curricula recommendation.

Governments have also realized the need for a workforce with knowledge and skills in the security area. In the US, an example of this is the National Initiative for Cybersecurity Education which is funded by various federal agencies with the mission to "Bolster formal cybersecurity education programs". In EU, there are various programs related to the boosting of awareness for security in education. ENISA (European Union Agency for Network and Information Security) has played an active part in raising awareness for the lack of opportunity for formal education in the area of Security and Privacy.

3 ICT Security Skills Gap Investigation

The objective of the survey is to investigate whether or not there are lacking ICT security skills in the industrial sectors at selected European regions and highlight recurring shortcomings across those regions. The investigation covered seven European regions and it was concluded in early 2016.

3.1 Investigation Methodology Logistics

The selected European regions were the **Be Wiser** consortium partners. Be Wiser (be-wiser.eu) is a project funded under the EU's Seventh Framework Programme for research, technological development and demonstration, investigation methodology and examines the organization and research challenges on Internet security in some of Europe's best-known Research Technology and Development (RTD) regions. Project partners participate under a Triple Helix Cluster (THC), formed to create synergies among SMEs, policy organizations, and academic/research institutes. The Be Wiser consortium partners consist of seven ICT THCs, drawn from different EU member states, namely: Ile-de-France region (France), Barcelona (Spain), Karlsruhe/Technologie Region (Germany), Cork/South West region (Ireland), Belfast (Northern Ireland), Slovenia, and Cyprus.

One of the Be Wiser activities was the investigation of the ICT security competences that are provided to meet the needs and requirements of the industry through education and training. The aim was not to conduct an in-depth analysis of the ICT skill shortage issues in Europe but rather to identify the main trends, based on both primary and secondary data. Qualitative primary data was collected from roundtable discussions organized in each region. Secondary data consisted of a literature review of existing reports/surveys on the ICT security competences in partner regions and the security skills and competences recommended by selected professional and other ICT related organizations.

Roundtable workshops were organized in each region with participants being key regional stakeholders such as research and educational institutions, large companies and SMEs from a wide range of sectors, and government and public policy agencies across the partner region. In this way, a holistic approach on issues and challenges pertinent to ICT security was adopted. Discussion points were drawn up in relation to two key areas of interest regarding ICT security, namely the Skills Pipeline and Research and Innovation Ecosystem. For the purpose of this study, the findings related to the Skills Pipeline area are examined. For each discussion point, participants were asked to: Define the problem or opportunity in regard to their region, propose solutions and/or discuss profits from the opportunity, and identify action points to address the issue in their region. The discussion points for the participants were reflecting the ICT labor force, thus covering the following: Current provision of skilled ICT graduates, attraction of skilled ICT talent from other regions or countries, work placement or apprentice system for students, up skilling and continuous professional development of existing ICT expertise, conversion of non ICT graduates, and curriculum development for ICT security courses.

3.2 Data Analysis

A summary of the findings of the roundtable workshops for the Be Wiser regions is presented in this section.

Starting with the Ile-de-France region, while 'standard' ICT competencies are rather easy to find, more specialized skills such as IT security skills are difficult to source and attract. There are several causes of this phenomenon:

- **Lack of current provision of skilled ICT security graduates and curriculum development.** In a general way, fewer young people are attracted by the ICT sector compared to the past. In addition, although the Ile-de-France region has a good training ecosystem related to the ICT domain, regarding the security domain, it is considered that an insufficient number of new security engineers are

trained to meet company needs. On one hand, the educational offering in the domains of wireless and Internet security is viewed as 'insufficient', 'too general' and not up to the standard required. On the other hand, students are not attracted by high tech specialized curriculums at a thematic Masters level and they prefer keeping more options open.

- **The attraction of skilled IT security talent problem.** Companies in the Ile-de-France region are struggling to attract qualified people. Numerous students and new graduates leave the region every year for the USA due to numerous reasons like higher salaries, better funded research, etc.
- **The ineffective Up-skilling & continuous professional development process**. In France employers have a legal right to offer CPD training. However, it appears that this right is complicated to implement in the case of very high skilled workers, or in the case of career change, and ongoing training is often only related to generic subjects. In addition, there are differences between large companies, able to provide internal training, and SMEs, which have to externalize, and which don't spend time and money for this.
- **Few partnerships exist between business and training providers.** Companies state that the existing trainings do not always meet their needs, in the content and in the form.

Moving on to the Barcelona/Catalonia region, the IT sector in Spain and in Catalonia is in good health. Barcelona is an attractive location for IT professionals: the brand of the city draws people and there is a good provision of IT skills in the region. Still, IT and security sectors face problems through the lack of qualified people to fill vacant ICT and security roles:

- **The decline in the number of ICT graduates over the last number of years.** Reasons for this phenomenon include demographic reasons, loss of popularity amongst students in technical degrees and a perception that a significant amount of effort is required to be awarded an honors degree.
- **The lack of communication, interaction and understanding between industry, HEI, and students.** There is a lack of understanding by HEIs of the profile requirements and overall market demands. Furthermore, students only make contact with industry when they almost complete their studies or after completion.
- **The difficulty to adapt the educational offer to meet industry needs.** The regional diagnosis enabled the identification of only five specialized degrees on this domain (related to 1830 students trained in ICT). In addition, lifelong learning of professionals to update their competencies is not very developed and security is not an easy topic to find outside of specific university courses**.**
- **The bigger challenge of training for SMEs.** There is a difference between large companies, which have integrated training program partnering with training centers or even considering in-house training, and SMEs, that find it difficult to train their workforce in regard to the lack of resources, expertise and co-ordination.
- **The low potential of conversion related to IT-security technical competences.** Conversion requires a significant investment in time and money and there is a perception that only those with college degrees would be able to adapt to the knowledge requirements of the IT sector.

The Karlsruhe/Technologie Region Karlsruhe region is one stronghold for the ICT sector in Germany. Firms are seeking growth, but are constrained by the difficulty to find suitably qualified employees:

- **Mobility and attractiveness of ICT graduates and professionals.** Karlsruhe is home to an excellent education and vocational training system containing high-quality universities and HEIs. Significant expertise in ICT courses exists with more than 5.600 students enrolled annually related informatics and similar subjects. However, few stay in the region, many leave for more 'attractive' regions like Munich or Berlin. Foreign students tend to leave when their studies are completed. In-

deed, the attractiveness of a region depends not only on its job market situation, but also on the housing situation and the quality of life for younger people.

- **Limited space for security in the IT training courses.** Some of the HEIs of the region offer single modules for IT security within the curricula of courses such as informatics, information engineering and industrial engineering. No specific course exists exclusively in 'IT security' and no specific degree for citizens aspiring to become an 'IT security manager'. Internet and wireless security form part of the courses offered across HEIs in Karlsruhe. Participation in these modules is not mandatory for students.
- **The difficulty for SMEs relating to traineeship up-skilling and Continuous Professional Development (CPD).** Traineeship and CPD are good ways for companies to have employees with the relevant competences, those meeting their industrial expectations. Despite the awareness about this necessity, start-ups and SMEs are often not able to offer traineeship or CPD. A major problem for SMEs to offer traineeship opportunities for students is the requirement of significant time and other resources for this purpose. In many cases, apprenticeships are shared because companies often don't have the resources to provide the entire apprenticeship.

In Cork/South West region, education in ICT related fields represents some 2090 students, of which some 50% are deemed to have followed training on wireless and Internet security as part of their studies. Education in ICT is mostly done through universities while education in security is mostly private (essentially performed by large companies). There is dependency by Cork ICT firms on recruiting IT and software professionals from abroad:

- **Adapt the current provision of ICT security education.** Many MNCs and SMEs require ICT professionals with a minimum of a 3-year experience and not necessarily graduates. Thus, the issue for employers and graduates in the region is to ensure that new graduates acquire the necessary experience and training. Industry suggests that practical skills are not given sufficient credit in universities, and instead the focus and acclaim is on research. However, the perception in industry is that it is better to hire people with practical experience rather than theoretical experience only. Developing work placements and traineeships offer many opportunities for putting classroom learning into practice and afford many opportunities for informal learning in the workplace. But organizing successful work placements requires considerable resources from both the HEIs and employers. This represents a barrier to SMEs taking on work placements due to the time and costs in organizing them.
- **Mismatch between 3rd-Level Courses and Industry requirements.** There is currently no undergraduate course on Internet security provided in the region. There is also a skills shortage in wireless security and wireless technology and in particular radio and radar design. HEIs have difficulty providing the number of graduates that industry needs, in a timely manner. By the time students complete a 4 year course and acquire 2 years' experience, technology trends are already changing.
- **Employment Retention for SMEs.** There is a difficulty in retaining employees for start-ups and SMEs. After graduates join a small company and gain experience, they are often poached by larger companies.
- **Attractiveness of ICT talents.** The tech sector in Dublin is widely known throughout Europe and is the European HQs for companies such as Twitter, Google, Microsoft and Facebook. Cork is not as widely known as a tech hub that reduces inward skilled migration increasing the local skills gap.
- **Lack of time and resources for up-skilling and CPD in Start-ups and SMEs**. Despite the number of up-skilling and CPD courses provided in the region through HEIs, up-skilling and CPD is considered a critical issue by SMEs. Academia acknowledges that it lacks sufficient funding and resourcing to meet the up-skilling needs of industry.

Most of the challenges faced by Ireland are also faced by Belfast/Northern Ireland Region: to find ICT professionals with a minimum of 3 years' experience and not necessarily graduates (and the need to develop work placements and traineeships), to retain employees for start-ups and SMEs because graduates have a preference for larger companies, the lack of attractiveness of the region due to its peripherality, the mismatch between 3rd-Level Courses and Industry requirements and the need for primary and secondary level support. Additionally, there is:

- **Lack of connection between skills providers and industry**. Despite the existence of Industry Liaison Panels tasked with bringing together the needs of industry within the capabilities and plans of the education sector, still there is a security skills gap. One of the significant initiatives in training is the MSc in cybersecurity launched in September 2014 by QUB-CSIT. A key differentiator of this MSc program is the opportunity to closely engage with CSIT industry partners
- **Lack of ICT conversion.** There is a lack of awareness on the broad range of employment within ICT from programming to sales to HR. ICT conversion courses in their current form are too broad and need to be categorized into different ICT disciplines.

Slovenia has a share of ICT specialists in the workforce of 2.6%, just below the EU average, and Slovenia compares favorably on the % of STEM (Science, Technology, Engineering and Mathematics) graduates, with 1.9% of Slovenians aged 20-29 years old holding a STEM degree. There are opportunities to meet ICT industry requirements:

- **The gap between the theoretical knowledge of ICT graduates and the experience companies require from their employees**. Regional stakeholders consider that there is not enough focus on wireless and Internet security in general and there is a lack of courses developed around internet security.
- **The failures of the apprentice system**. The main issue emphasized was that students who start working during their studies usually experience serious delays in graduation or they don't graduate. Many smaller companies view students only as a resource and are not interested in their long-term education and skills development. The apprentice system is very complex from an administrative perspective. Therefore, companies rarely decide to make use of it. Another issue is related to the time it takes to introduce students to the work system of individual companies.
- **The under-development of life-long learning.** There is a number of experienced ICT professionals who work on specific technologies for a long period of time and have limited time for upskilling. A significant challenge relates to how such staff upgrade their knowledge and allow them the opportunity to compete in the market with newly adopted skills. Only a small number of upskilling and professional development courses are available in Slovenia because the market is small.

In Cyprus the unemployment rate among young ICT graduates is high compared to three years ago. There is currently a surplus of qualified ICT graduates which forces many to seek employment opportunities abroad or, those who study abroad, to stay and work abroad. In addition, industry representatives believe that ICT graduates suffer from a lack of practical experience and business mind-set among academics, and the title 'Qualified' is usually coupled with unreal remuneration expectations (for Cyprus companies) from candidates:

- **Mismatch between curricula and ICT industry needs.** Regional ICT companies stated that the curricula of local universities in this field do not currently meet the needs of the ICT industry and that most ICT related university programs are still too theoretical.

- **The employment paradox**. Due to the economic situation in Cyprus, ICT graduates experience a high unemployment rate and many local ICT professionals cannot get the experience requested by employers due to the lack of companies that can offer that kind of experience. Thus, a number of local ICT companies attempt to attract experienced ICT professionals from other countries, but this is not a large number. At the same time, skilled ICT talent (qualified graduates) and experienced ICT professionals from Cyprus prefer to emigrate for improved employment prospects.
- **The lack of formal work placement or apprenticeship programs between industry and academia**. Universities are looking for opportunities for student placements and apprentice internships, but there is a lack of internship availability and/or interest from the industrial sector, and no formal programs are in place. Usually the work placements are optional and it is up to the students to make arrangements.
- **The cost of professional certifications.** One of the top priorities of many ICT professionals is the acquisition of professional certifications. As these certifications frequently appear within ICT related vacancy announcements, their possession increases employment opportunities and enhances career development prospects.

4 Narrowing the Security Skills Gap

Taking into consideration the findings from the roundtable workshops, the market needs on ICT security, and the educational approach on ICT security, it is evident that all stakeholders recognize the importance of security and at the same time confirm the existence of a gap between market-oriented security skills and educational competences that mostly focus on theoretical aspects. However, the responses from the various regions indicate differences in the security needs and the available training in those areas. Thus, it could be the case that 'one-size fits all' approach on narrowing the gap does not apply here. Most likely, each region will need to adapt/extend common guidelines to its specific needs. Having this in mind, we are proposing a framework that supports a basic taxonomy of three influential factors in narrowing the security skills gap: major pillars of an education and training program, interested parties, and type of the regional industry. These are illustrated in Figure 1.

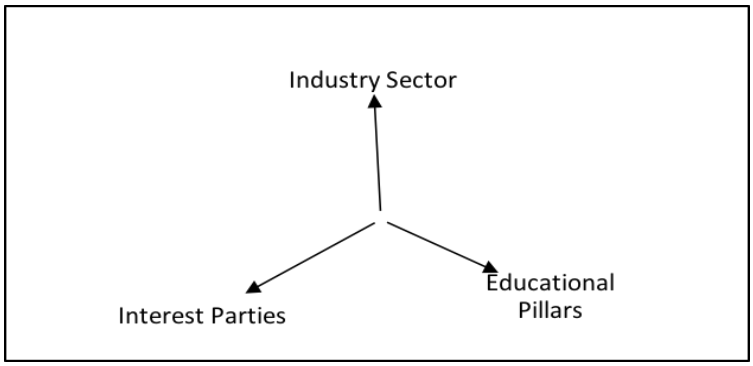

Figure 1: Influential Factors in Narrowing Security Skills Gap

The first factor is the educational approach on security education. Security is a relatively new key knowledge area that evolves rapidly and has an impact on other 'mature' key knowledge areas. For example, secure programming, security software engineering, privacy by design are examples of security being an integral part of mature areas such as programming principles and system design. In addition, the introduction of disruptive technologies such as mobile technologies affects all key knowledge areas that need to address the new realities. The power consumption, for instance, is a new constraint

that affects not just security design but also operating system design. It is the task of HEIs to provide students, who constitute the future labor force, with a 'dynamic' skillset not only to start their professional careers but also to be able to remain relevant in the area by improving their competences/skills.

A dynamic skillset is the driving force behind narrowing the security skills gap. We have identified three broad pillars of the knowledge, skills, and competences of a tertiary education in security, which yield a dynamic skillset:

- Deep and thorough knowledge of the theoretical aspects of ICT security
- Basic skillset using current security technologies, techniques, and best practices
- Ability to absorb new knowledge and cultivate new skills and competences.

The second factor is the interest parties and their competing interest in placing more emphasis on one or two pillars, at the expense of the remaining one(s). The interest parties identified are academics, SME and start-ups, and large enterprises along with MNC. Figure 2 illustrates the relationship between the three pillars and the interest groups.

The last factor is the type of the industry sector. Different regions will have different needs depending on the type of industry they have. Three broad industry sectors (related to ICT professionals) can be defined:

- Research & development (R&D) company/laboratory
- IT company that provides consulting/testing services regarding IT infrastructures
- Security professionals administrating companies' IT infrastructure on a daily basis.

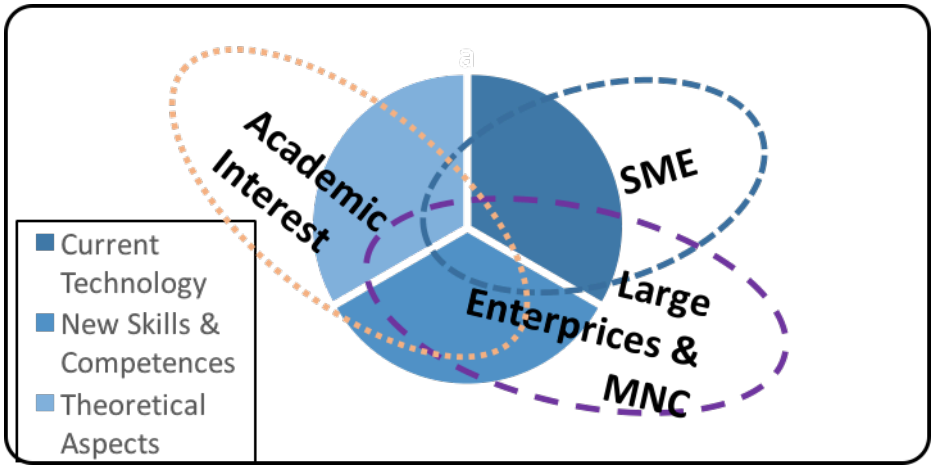

Figure 2: Educational Pillars and Interest Groups

As observed from the respondents' responses, different regions have different needs and the education sector in the region needs to consider them in order to cater the required market skills. For instance, in the Belfast region there are needs by the R&D industry, hence the emphasis would be on the theoretical pillar, whereas in the Slovenia region there is a lack of ICT professionals, thus more focus could be given on the current technology pillar. Narrowing the gap primarily falls on the shoulders of the educational sector, as it is the one that supplies the work force. Depending on the type of the regional industry, focus could be shifted towards the pillars that would best cater the industry needs. Qualitative and quantitative studies must be conducted to profile the regional industry and then customize the educational programs to satisfy the security skills and competences required by the region. The profile construction is a dynamic process that needs to be executed frequently. If a region is too specialized, rapid and disruptive changes, common in the ICT industry, may result in obsolete specialized exper-

tise. On-going adaptation of curricula must be aligned with the regional industry expectations and follow the rapid changes in ICT security. More details are given on the three pillars in relation to the other two factors.

4.1 Deep and Thorough Knowledge of Theoretical Aspects

The ICT field is part of the STEM disciplines and as such it requires a strong background on fundamental theory courses and mathematics. In order to protect an IT infrastructure, one needs to be familiar with its design and implementation strategies, hence a deep knowledge on automata theory, discrete mathematics, graph theory, logic, and statistics is of paramount importance. The breadth and depth of this pillar compared to the other two pillars depend on the needs on the interest groups and the industrial sector of the region (and the state needs as a whole).

In general, academics tend to be in favor of theoretical courses that prepare students for postgraduate studies, as there is the pressure of *publish or perish* in the academic circles. Well-trained graduate students with strong foundations could positively contribute in the research of academics, which in most cases is basic research with some/or no applied nature. Furthermore, one could argue that the content of theoretical content stays fairly static compared to applied ones, meaning that no frequent course update is required.

The R&D industry shares the academic interests. There is a difference in the expectation of the R&D industry compared to the 'pure' academics in that the R&D emphasizes the technical understanding than basic theory. The remaining two industries (consultants, practitioners) focus more on the latest technologies, tools and techniques as those are the important aspects for delivering their tasks. Even in this case, it could be argued that the exposure to the theoretical fields during their academic studies provided the training needed to quickly adapt and learn new tools and techniques. And as the ICT field is ever changing, this ability might be one of the most important skill. Quoting Einstein, *'Education Is What Remains After You Have Forgotten Everything You Learned In School'*.

4.2 Basic Skillset using Current Security Technologies, Techniques, and Best Practices

It is evident from the roundtable discussions that industry needs are not fully covered by the HEIs. Recent graduates do not know the latest technologies in their fields, and this lack of skills/competences is often attributed to the HEI curricula and academics: they are too theoretical without providing the students with a basic skillset as required by the industry.

Academics committed to both research and teaching may find it difficult to balance excelling in research and keeping up with the latest technologies in their field. It takes a lot of effort, resources, and expenses to continuously training faculty to know all the ins-and-outs of specific platforms and software. Academics prefer to convey to students general problem-solving methodologies rather than focusing on a specific technology (focus on the third pillar below). In this way the students are expected to make the transition from theoretical to practical on their own. In addition, research contributions carry more weight than teaching contributions in the academic community, and therefore it is not in the faculty's best interest to stay updated with all cutting edge technologies. In some educational institutes, this problem is somewhat alleviated with having graduate students being responsible of laboratory work. As a general rule, graduate students keep themselves up-to-date with current technologies.

A basic skillset is required by the industrial sector, but there are conflicting approaches on the dynamic nature of the skillset. On one hand, there are employers who are looking for employees that have specific skills and competences using specific platforms and/or software. The main advantage is the immediate utilization of the employee, skipping the learning phase. However, as soon as the platform is outdated/upgraded, training may be needed with a long learning curve. On the other hand, there are

employers who focus more on the employee's ability to quickly adapt to a new platform and/or software. The employer invests at the beginning on the employee's initial training on familiarizing with the company's technologies but saves time later on when upgrades or new technologies are introduced.

As far as the academic curricula are concerned, the course contents do not always align with the practical approach of the industrial needs as there is little or no consultation with the industry during course development. However, the rapid changes in the ICT field prompted the HEIs to shift from generic programs to more specialized ones. The generic computer science degree has already been split into new fields, like Computer Engineering, MIS (Management Information Systems), Software Engineering, with their own curriculum guidelines and professional interest organizations. At the postgraduate level, HEI are offering specialized degrees like, MSc in Cyber Security, MSc in Web Development, MSc in Mobile Systems, etc. Still, the specialized nature of programs does not necessarily imply a more practical approach.

Specialized security skills could be obtained through training outside HEIs. Professional certifications such as Cisco certificates and Microsoft training programs attempt to fill the gap, but only particular parts of it that it is in their best interest. Training programs target not only students who wish to specialize in a specific platform but also current employees that need to enhance their skills as new platforms and technologies are introduced. Professional certifications are not competing with HEIs but they are rather complimenting each other.

4.3 Absorb new Knowledge and Cultivate New Skills and Competences

This is the most challenging task for an educator and it highly depends on the individual and his/her ability of learning. This is the recursive nature of learning where a student enriches his/her basic skillset and competences on his/her own, usually through practical experience. For example, a student familiar with wired security protocols should be able to adopt to wireless security protocols, given the proper educational training.

The weight that companies place on this pillar depends on many factors. Large enterprises in good financial situation may consider this as one of the most important hiring criteria as a newly-hired employee is a long term investment. Start-ups and smaller companies, usually with a small work force that may need to wear 'multiple hats' within the company, do not have the luxury of extended training as they count on the productivity of the new employee from day one. Hence, they may put less emphasis on this pillar and more on the previous pillar.

The ability to absorb new knowledge, but at different levels, is essentials in all three sectors of industry. The researcher and developer need to absorb new knowledge at a deeper level, like development tools, technologies, and computer/systems architectures. The consultant concentrates on being able to have a broad knowledge of different tools and software systems as to recommend which will work best with a specific organization. Last, the ICT professional should know all the ins-and- outs of the specific tools and software systems that he/she is managing.

5 Conclusion

The rapid evolution of the information society is transforming the ICT sector as a supporting critical infrastructure, whose interruption could have severe impact on numerous aspects of life such as business, education, social, to just name a few. It is of paramount importance to protect and secure network systems and assets from intentional attacks that would cause disruption of network services. Highly qualified security professionals alleviate the threat of compromising system networks and gaining unauthorized access to data. However, it has been observed that the market needs on security skills and competences do not always align with the ones cultivated by the educational sector. This misalign-

ing creates a security skills gap that is exploited by malicious parties, leaving enterprises unprotected and vulnerable to cyber attacks.

The aim of this research work was to investigate the security skills gap in seven EU regions and suggest an approach to narrow it. The survey findings indicated the difficulty to devise a common set of best practices that would apply to all as the various industry sectors had different focus areas. Hence, a framework was devised that supports a basic taxonomy of the various interested parties (academics, MNC, SME, startup), the security professional's work function (R&D, consultants, administrator), and the major pillars of an education and training program (theory, basic skillset, adaptability to new technologies). Depending on the type of the regional industry, focus could be shifted towards the pillars that would best cater the industry needs. Qualitative and quantitative studies must be conducted to profile the regional industry and then customize the educational programs to satisfy the security skills and competences required by the region. The profile construction is a dynamic process that needs to be executed frequently.

Acknowledgment

This work was supported by the EU FP7 Be Wiser project (Grant No: 319907). The authors would like to thank the Be Wiser consortium members for conducting the roundtable workshops in their regions and for their valuable feedback.

References

Cisco (2014). Cisco 2014 Annual Security Report. White Paper URL: http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf (visited on 20/05/2016).

Dodge, R. (2013). "Information Assurance and Security in the ACM/IEEE CS2013", In: *Proceedings of the 8th IFIP WG 11.8 World Conference on Information Security Education, WISE 8,* Auckland, New Zealand. Ed. by R. Dodge and L. Futcher. Springer Berlin Heidelberg. P. 48 – 57.

Foster and Sullivan (2013). Critical Times Demand Critical Skills: An analysis of the skills gap in information security, URL: https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/GISWS-Skills-Gap-Analysis.pdf (visited on 20/05/2016).

Kennedy, D. (2015). Q2 2015 - Voice of the Enterprise: Information Security, Advisory Report. URL: https://451research.com/report-long?icid=3472 (visited on 20/05/2015)

National Initiative for Cybersecurity Education (NICE) (2013). The National Cybersecurity Workforce Framework. http://csrc.nist.gov/nice/framework/ (visited on 20/05/2015)

Pauna, A., Linares, S., Paredes, I., Valiente, J., Pilar, J., Bruna, T., Martínez, S., and Huistra, A. (2014). "Certification of Cyber Security skills of ICS/SCADA professionals." Technical Report TP-07-14-040-EN-N. European Union Agency for Network and Information Security (ENSIA).

Libicki, M., Senty, D., and Pollak, J. (2014). Hackers Wanted: An Examination of the Cybersecurity Labor Market. Santa Monica, CA: RAND Corporation. URL: http://www.rand.org/pubs/research_reports/RR430.html. (visited on 20/05/2016)

Suby, M., and Dickson (2015). "The 2015 (ISC)2 Global Information Security Workforce Study". Foster & Sullivan White Paper, URL: https://www.isc2cares.org/industryresearch/gisws/.

Wadlow, T. (2015). *Top 10 IT Skills in Demand for 2015*. URL: http://www.businessrevieweurope.eu/technology/380/Top-10-IT-Skills-in-Demand-for-2015/ (visited on 20/05/2016).

World Economic Forum (2014). *Global Risks 2014*. URL: http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf (visited on 20/05/2016).